NSE8_812 Q&As

Network Security Expert 8 Written Exam

Pass Fortinet NSE8_812 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/nse8_812.html

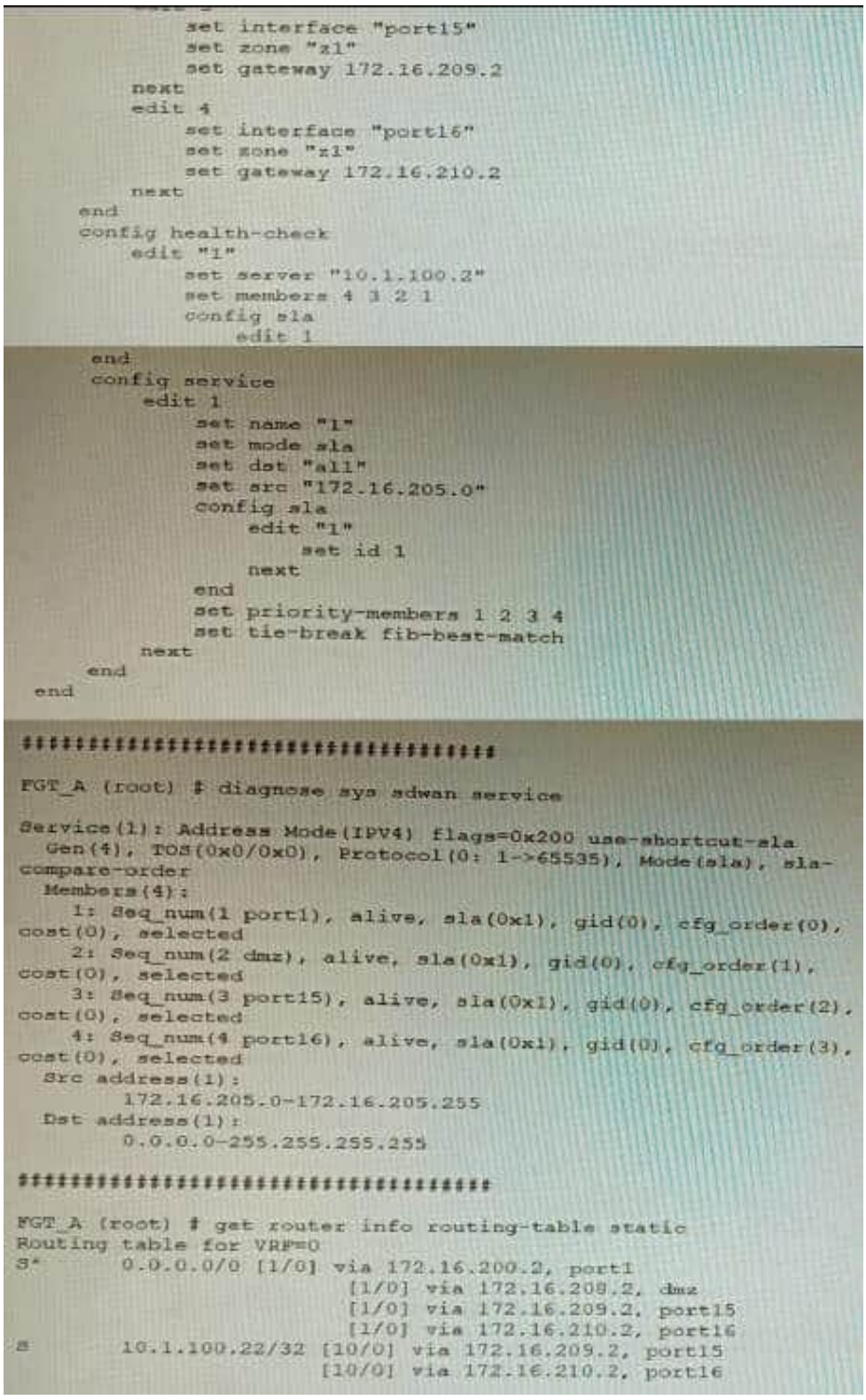
100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Refer to the exhibit showing an SD-WAN configuration. According to the exhibit, if an internal user pings 10.1.100.2 and 10.1.100.22 from subnet 172.16.205.0/24, which outgoing interfaces will be used?



A. port16 and port1

B. port1 and port1

C. port16 and port15

D. port1 and port15

Correct Answer: A

Explanation: According to the exhibit, the SD-WAN configuration has two rules: one for traffic to 10.1.100.0/24 subnet, and one for traffic to 10.1.100.16/28 subnet. The first rule uses the best quality strategy, which selects the SD-WAN member with the best measured quality based on performance SLA metrics. The second rule uses the manual strategy, which specifies port1 as the SD-WAN member to select. Therefore, if an internal user pings 10.1.100.2 and 10.1.100.22 from subnet 172.16.205.0/24, the outgoing interfaces will be port16 and port1 respectively, assuming that port16 has the best quality among the SD- WAN members.
References:https://docs.fortinet.com/document/fortigate/6.2.14/cookbook/218559/configurin g-the-sd-wan-interface

QUESTION 2

Refer to the exhibit.

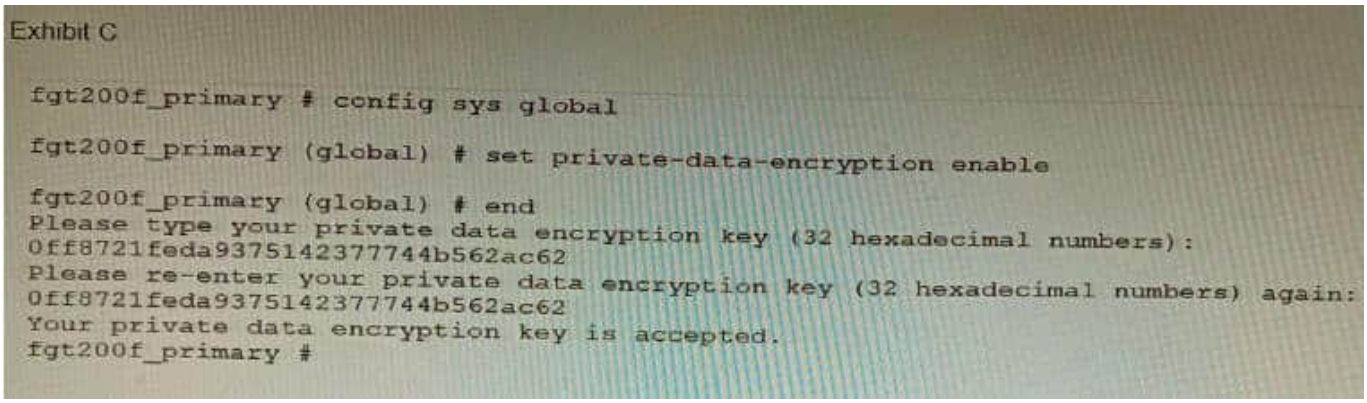


Exhibit C

```
fgt200f_primary # config sys global

fgt200f_primary (global) # set private-data-encryption enable

fgt200f_primary (global) # end
Please type your private data encryption key (32 hexadecimal numbers):
0ff8721feda93751423777744b562ac62
Please re-enter your private data encryption key (32 hexadecimal numbers) again:
0ff8721feda93751423777744b562ac62
Your private data encryption key is accepted.
fgt200f_primary #
```

A customer has deployed a FortiGate 200F high-availability (HA) cluster that contains and TPM chip. The exhibit shows output from the FortiGate CLI session where the administrator enabled TPM.

Following these actions, the administrator immediately notices that both FortiGate high availability (HA) status and FortiManager status for the FortiGate are negatively impacted.

What are the two reasons for this behavior? (Choose two.)

A. The private-data-encryption key entered on the primary did not match the value that the TPM expected.

B. Configuration for TPM is not synchronized between FortiGate HA cluster members.

C. The FortiGate has not finished the auto-update process to synchronize the new configuration to FortiManager yet.

D. TPM functionality is not yet compatible with FortiGate HA D The administrator needs to manually enter the hex private data encryption key in FortiManager

Correct Answer: AB

Explanation: The two reasons for the negative impact on the FortiGate HA status and FortiManager status after enabling TPM are: The private-data-encryption key entered on the primary unit did not match the value that the TPM expected. This could happen if the TPM was previously enabled and then disabled, and the key was changed in between. The TPM will reject the new key and cause an error in the configuration synchronization. Configuration for TPM is not synchronized between FortiGate HA cluster members. Each cluster member must have the same private-data-encryption key to form a valid HA cluster and synchronize their configurations. However, enabling TPM on one unit does not automatically enable it on the other units, and the key must be manually entered on each unit. To resolve these issues, the administrator should disable TPM on all units, clear the TPM data, and then enable TPM again with the same private-data-encryption key on each unit. References:
https://docs.fortinet.com/document/fortigate/6.4.0/cookbook/103437/inbound-ssl- inspection
https://docs.fortinet.com/document/fortigate/6.4.0/cookbook/103438/application- detection-on-ssl-offloaded-traffic

QUESTION 3

A customer\\'s cybersecurity department needs to implement security for the traffic between two VPCs in AWS, but these belong to different departments within the company. The company uses a single region for all their VPCs.

Which two actions will achieve this requirement while keeping separate management of each department\\'s VPC? (Choose two.)

A. Create a transit VPC with a FortiGate HA cluster, connect to the other two using VPC peering, and use routing tables to force traffic through the FortiGate cluster.

B. Create an 1AM account for the cybersecurity department to manage both existing VPC, create a FortiGate HA Cluster on each VPC and IPSEC VPN to force traffic between the VPCs through the FortiGate clusters

C. Migrate all the instances to the same VPC and create 1AM accounts for each department, then implement a new subnet for a FortiGate auto-scaling group and use routing tables to force the traffic through the FortiGate cluster.

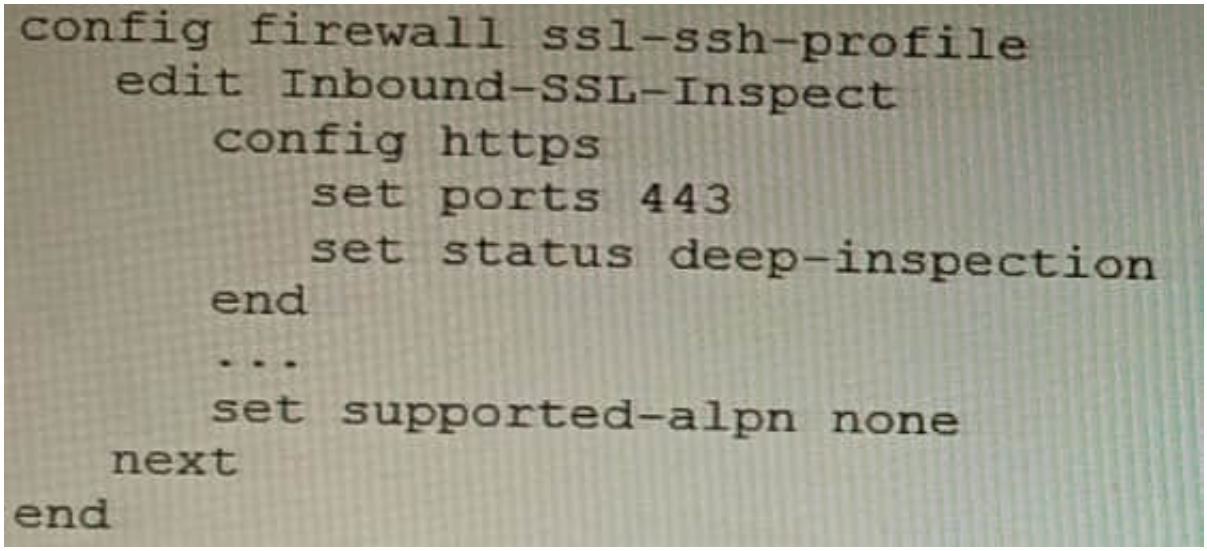
D. Create a VPC with a FortiGate auto-scaling group with a Transit Gateway attached to the three VPC to force routing through the FortiGate cluster

Correct Answer: AD

Explanation: To implement security for the traffic between two VPCs in AWS, while keeping separate management of each department\\'s VPC, two possible actions are: Create a transit VPC with a FortiGate HA cluster, connect to the other two using VPC peering, and use routing tables to force traffic through the FortiGate cluster. This option allows the cybersecurity department to manage the transit VPC and apply security policies on the FortiGate cluster, while the other departments can manage their own VPCs and instances. The VPC peering connections enable direct communication between the VPCs without using public IPs or gateways. The routing tables can be configured to direct all inter-VPC traffic to the transit VPC. Create a VPC with a FortiGate auto-scaling group with a Transit Gateway attached to the three VPCs to force routing through the FortiGate cluster. This option also allows the cybersecurity department to manage the security VPC and apply security policies on the FortiGate cluster, while the other departments can manage their own VPCs and instances. The Transit Gateway acts as a network hub that connects multiple VPCs and on-premises networks. The routing tables can be configured to direct all inter-VPC traffic to the security VPC. References:
https://docs.fortinet.com/document/fortigate-public-cloud/7.2.0/aws-administration- guide/506140/connecting-a-local-fortigate-to-an-aws-vpc-vpn https://docs.fortinet.com/document/fortigate-public-cloud/7.0.0/sd-wan- architecture-forenterprise/166334/sd-wan-configuration

QUESTION 4

Refer to the CLI configuration of an SSL inspection profile from a FortiGate device configured to protect a web server:



Based on the information shown, what is the expected behavior when an HTTP/2 request comes in?

A. FortiGate will reject all HTTP/2 ALPN headers.

B. FortiGate will strip the ALPN header and forward the traffic.

C. FortiGate will rewrite the ALPN header to request HTTP/1.

D. FortiGate will forward the traffic without modifying the ALPN header.

Correct Answer: A

Explanation: Thesupported-alpnparameter is set tohttp1.1in the SSL inspection profile. This means that the FortiGate will only accept HTTP/1.1 traffic. Any HTTP/2 traffic will be rejected.

The following is the relevant documentation from Fortinet:

Thesupported-alpnparameter specifies the list of ALPN protocols that the FortiGate will accept. If the client requests a protocol that is not in this list, the FortiGate will reject the connection.

The default value for thesupported-alpnparameter isall. This means that the FortiGate will accept any ALPN protocol that the client requests. To reject all HTTP/2 traffic, set thesupported-alpnparameter tohttp1.1. Source: https://

docs.fortinet.com/document/fortigate/7.0.0/new-features/710924/http-2- support-in-proxy-mode-ssl-inspection

QUESTION 5

You are deploying a FortiExtender (FEX) on a FortiGate-60F. The FEX will be managed by the FortiGate. You anticipate high utilization. The requirement is to minimize the overhead on the device for WAN traffic.

Which action achieves the requirement in this scenario?

A. Add a switch between the FortiGate and FEX.

B. Enable CAPWAP connectivity between the FortiGate and the FortiExtender.

C. Change connectivity between the FortiGate and the FortiExtender to use VLAN Mode

D. Add a VLAN under the FEX-WAN interface on the FortiGate.

Correct Answer: C

Explanation: VLAN Mode is a more efficient way to connect a FortiExtender to a FortiGate than CAPWAP Mode. This is because VLAN Mode does not require the FortiExtender to send additional control traffic to the FortiGate. The other options are not correct.

A. Add a switch between the FortiGate and FEX. This will add overhead to the network, as the switch will need to process the traffic. B. Enable CAPWAP connectivity between the FortiGate and the FortiExtender. This will increase the overhead on the FortiGate, as it will need to process additional control traffic.

D. Add a VLAN under the FEX-WAN interface on the FortiGate. This will not affect the overhead on the FortiGate.